Amendments to the Specification:

Please replace the paragraph beginning on page 1, line 12 with "This patent..." and ending on page 1, line 15 with "...System" with the following amended paragraph:

This patent application relates to and claims priority from U.S. Provisional Patent Application No. 60/298,770, filed Jun. 15, 2001, which is pending and application Ser. No. [[_____]] 09/944,333 filed Aug. 30, 2001, entitled "Secure Selective Sharing of Account Information on an Internet Information Aggregation System."

Please replace the paragraph beginning on page 6, line 18 with "Figure 10..." and ending on page 6, line 19 with "...web-site" with the following amended paragraph:

Figures 10A-10B are [[is]] a flow chart of one preferred embodiment of a routine for getting data from a web-site.

Please replace the paragraph beginning on page 15, line 17 with "Figure 10..." and ending on page 16, line 8 with "...eliminated" with the following amended paragraph:

Figures 10A and 10B show [[is]] a flow chart of one preferred embodiment of a routine for getting data from an institute or web-site. Turning to Figure 8B, the routine of Figure 10A is initiated when data is not available for a particular institute/web-site (block 460). If data is not

available, the system initiates the routine of Figure 10A. The routine of Figure 10A may be initiated in various ways and at different times, e.g. upon initial login, at periodic intervals, upon population of monitor, or when the user selects "Refresh" 500. The system retrieves an institute/web-site name 504 from the user institute/web-site account database ~~5048~~ 508. The system retrieves the user's account ID from database 520 and decrypts the user's ID 512 using an ID decryption key 516. The system further retrieves the user's PIN or password from database 528 and decrypts the PIN/password 520 using a PIN/password decryption key 524. The system retrieves the institute/web-site's script 536 from institute script knowledge database 532. The system then executes a data aggregation routine such as a PDE routine 600 of Figure 10B. A preferred PDE routine is described below and in Figure 11A, 11B and 11C. When the PDE routine 600 is complete, the system retrieves the data 540 from the institute/web-site. Similarly data could be aggregated with ~~OFK, IFK~~, OFX, IFX, QIF, XML, or other data interchange standards or proprietary methods as illustrated in Figure 10B. The system normalizes the data 544 (e.g. round off decimal places and otherwise place the data in a format acceptable for display on the view page 20). The system encrypts the data 548 using a user data encryption key 552. The system then stores the data 556 in the user's data store 472. Once the data for the institute or web-site is stored in the data store 472, the data can be retrieved by the system using the routine shown in blocks 468-492 of Figure 8. When retrieving non-confidential data (e.g. for the weather monitor 10), the encryption and decryption steps can be eliminated.

Please replace the paragraph beginning on page 16, line 11 with "Figure 11..." and ending on page 16, line 29 with "...(pages)" with the following amended paragraph:

Figures 11A-11C show [[is]] a flow chart of one preferred embodiment of a routine for PDE. As mentioned above, PDE is a technique used in information aggregation systems to gather confidential data from web-sites. Referring back to Figures 10A and 10B, the PDE function is initiated while gathering data from a web-site. At block 536 of Figure 11A, the system obtains information about the institute/web-site (e.g. url, login, and name of institute) from the institute script knowledge base 532. The system retrieves the user's account ID or user name from database 616 and decrypts the user's ID using an ID decryption key 612. The system further retrieves the user's PIN or password from database 624 and decrypts the PIN/password using a PIN/password decryption key 620. The knowledge module then connects to the website from which data is to be collected 644. It then identifies the connection type supported by the website server 656. Some sites communicate using normal HTTP protocol while others use secure HTTP (HTTPS) using SSL encryption. If SSL encryption is to be used 660, the corresponding SSL certificate for the server is loaded 668 and a secure socket is opened by the knowledge module 676. While opening the secure socket, the knowledge module has to select the most appropriate encryption and decryption algorithms supported by the server 672. If the server supports normal HTTP communication, an ordinary socket connection is established between the knowledge module and the corresponding website server. The knowledge module transmits the login information to the website over the socket connection 680. The login session information and cookies etc. are accepted by the knowledge module 684. This session information and cookies are to be sent back to the server to access other resources (pages).

Please replace the paragraph beginning on page 17, line 1 with "The knowledge..." and ending on page 17, line 5 with "...database 708" with the following amended paragraph:

The knowledge module accesses the HTML pages containing the required data using the session information and cookies over the socket connection 690. The response from the server is passed and the required data extracted 694. More pages are requested from the server if data has to be collected from them 696. When all the required data has been collected the data is encrypted 704 using the encryption key for the user and is then stored in the database 708 for the specific User Account Data 712.

Please replace the paragraph beginning on page 19, line 19 with "Figure 13C..." and ending on page 20, line 1 with "...990" with the following amended paragraph:

Figure 13C is a flow chart for the process of accessing the aggregated information using a mobile device. The information to be accessed through the mobile device is set up in the manner explained in the previous section. The process starts when the user invokes the application on a mobile device 952. The mobile device sends the server a request for the welcome page of the web server of the information aggregation system. The server recognizes the type of device from the request 956, and sends the corresponding welcome page 960. On the welcome page, the user is prompted to enter his user ID and the mobile password [[904]] 964. The user ID and password entered by the user is validated [[908]] 968. After validating the password 972, if the validation fails an error message is displayed 976, or a list of accounts (information sources which are

selected by the user to be accessed through the mobile device) is displayed 980. The user selects the information that he desires to view 984. Details about the selected account are displayed in a format that suits the mobile device 988. After viewing the information, the user decides to view another account 992 or logs out of the application [[990]] 996.